This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This document defines two EAP extended key usage values and a public key certificate extension to carry Wireless LAN (WLAN) System Service identifiers (SSIDs).
1. Introduction

Several Extensible Authentication Protocol (EAP) [EAP] authentication methods employ X.509 public key certificates. For example, EAP-TLS [EAP-TLS] can be used with PPP [PPP] as well as IEEE 802.1X [802.1X]. PPP is used for dial-up and VPN environments. IEEE 802.1X defines port-based, network access control, and it is used to provide authenticated network access for Ethernet, Token Ring, and Wireless LANs (WLANs) [802.11].

Automated selection of certificates for PPP and IEEE 802.1X clients is highly desirable. By using certificate extensions to identify the intended environment for a particular certificate, the need for user input is minimized. Further, the certificate extensions facilitate the separation of administrative functions associated with certificates used for different environments.

IEEE 802.1X can be used for authentication with multiple networks. For example, the same wireless station might use IEEE 802.1X to authenticate to a corporate IEEE 802.11 WLAN and a public IEEE 802.11 "hotspot." Each of these IEEE 802.11 WLANs has a different network name, called Service Set Identifier (SSID). If the network operators have a roaming agreement, then cross realm authentication allows the same certificate to be used on both networks. However, if the networks do not have a roaming agreement, then the IEEE 802.1X client needs select a certificate for the current network environment. Including a list of SSIDs in a certificate extension facilitates automated selection of an appropriate X.509 public key certificate without human user input.

1.1. Conventions Used In This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [STDWORDS].

1.2. Abstract Syntax Notation

All X.509 certificate [X.509-97] extensions are defined using ASN.1 [X.208-88, X.209-88].

2. EAP Extended Key Usage Values

RFC 3280 [PROFILE] specifies the extended key usage X.509 certificate extension. The extension indicates one or more purposes for which the certified public key may be used. The extended key usage extension can be used in conjunction with key usage extension, which indicates the intended purpose of the certified public key. For
example, the key usage extension might indicate that the certified public key ought to be used only for validating digital signatures.

The extended key usage extension definition is repeated here for convenience:

\[
\text{id-ce-extKeyUsage OBJECT IDENTIFIER ::= \{id-ce 37\}}
\]

\[
\text{ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId}
\]

\[
\text{KeyPurposeId ::= OBJECT IDENTIFIER}
\]

This specification defines two KeyPurposeId values: one for EAP over PPP, and one for EAP over LAN (EAPOL). Inclusion of the EAP over PPP value indicates that the certified public key is appropriate for use with EAP in the PPP environment, and the inclusion of the EAPOL value indicates that the certified public key is appropriate for use with the EAP in the LAN environment. Inclusion of both values indicates that the certified public key is appropriate for use in either of the environments.

\[
\text{id-kp OBJECT IDENTIFIER ::= \{ iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) 3 \}}
\]

\[
\text{id-kp-eapOverPPP OBJECT IDENTIFIER ::= \{ id-kp 13 \}}
\]

\[
\text{id-kp-eapOverLAN OBJECT IDENTIFIER ::= \{ id-kp 14 \}}
\]

The extended key usage extension may, at the option of the certificate issuer, be either critical or non-critical. If the extension is marked as critical, then the certified public key MUST be used only for the purposes indicated. However, if the extension is marked as non-critical, then extended key usage extension MAY be used to support the location of an appropriate certified public key.

If a certificate contains both a critical key usage extension and a critical extended key usage extension, then both extensions MUST be processed independently, and the certificate MUST only be used for a purpose consistent with both extensions. If there is no purpose consistent with both critical extensions, then the certificate MUST NOT be used for any purpose.

3. WLAN SSID Extension

The Wireless LAN (WLAN) System Service identifiers (SSIDs) certificate extension is always non-critical. It contains a list of SSIDs. When more than one certificate includes an extended key usage extension indicating that the certified public key is appropriate for
use with the EAP in the LAN environment, the list of SSIDs MAY be
used to select the correct certificate for authentication in a
particular LAN environment.

The WLAN SSID extension is identified by id-pe-wlanSSID.

\[
\text{id-pe OBJECT IDENTIFIER ::= \{ iso(1) identified-organization(3)
\quad dod(6) internet(1) security(5) mechanisms(5) pkix(7) 1 \}}
\]

\[
\text{id-pe-wlanSSID OBJECT IDENTIFIER ::= \{ id-pe 13 \}}
\]

The syntax for the WLAN SSID extension is:

\[
\text{SSIDList ::= SEQUENCE SIZE (1..MAX) OF SSID}
\]

\[
\text{SSID ::= OCTET STRING (SIZE (1..32))}
\]

4. Security Considerations

The procedures and practices employed by the certification authority
(CA) MUST ensure that the correct values for the extended key usage
extension and SSID extension are inserted in each certificate that is
issued. Relying parties may accept or reject a particular
certificate for an intended use based on the information provided in
these extensions. Incorrect representation of the information in
either extension could cause the relying party to reject an otherwise
appropriate certificate or accept a certificate that ought to be
rejected.

5. References

5.1. Normative References

[PROFILE] Housley, R., Polk, W., Ford, W. and D. Solo, "Internet
X.509 Public Key Infrastructure: Certificate and
Certificate Revocation List (CRL) Profile", RFC 3280,
April 2002.

[STDWORDS] Bradner, S., "Key words for use in RFCs to Indicate

Syntax Notation One (ASN.1). 1988.

Encoding Rules for Abstract Syntax Notation One (ASN.1).
5.1. Informative References


[802.11] IEEE Std 802.11, "Wireless LAN Medium Access
Control (MAC) and Physical Layer (PHY) Specifications",
1999.

[802.1X] IEEE Std 802.1X, "Port-based Network Access Control",

[EAP] Blunk, L. and J. Vollbrecht, "PPP Extensible

[EAPTLS] Aboba, B. and D. Simon, "PPP EAP TLS Authentication

[PPP] Simpson, W., Editor, "The Point-to-Point Protocol (PPP)",

6. ASN.1 Module

WLANCertExtn

{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-wlan-extns(24) }  

DEFINITIONS IMPLICIT TAGS :=
BEGIN

-- OID Arcs

id-pe  OBJECT IDENTIFIER  ::=  
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) 1 }  

id-kp  OBJECT IDENTIFIER  ::=  
{ iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) 3 }  

-- Extended Key Usage Values

id-kp-eapOverPPP  OBJECT IDENTIFIER  ::=  ( id-kp 13 )  

id-kp-eapOverLAN OBJECT IDENTIFIER  ::=  ( id-kp 14 )
-- Wireless LAN SSID Extension

id-pe-wlanSSID  OBJECT IDENTIFIER  ::=  { id-pe 13 }

SSIDList  ::=  SEQUENCE SIZE (1..MAX) OF SSID

SSID  ::=  OCTET STRING (SIZE (1..32))

END

7. Author’s Address

Russell Housley
RSA Laboratories
918 Spring Knoll Drive
Herndon, VA 20170
USA
rhousley@rsasecurity.com

Tim Moore
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
USA
timmoore@microsoft.com
8. Full Copyright Statement

Copyright (C) The Internet Society 2002. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.